CCC:MKC
F.#2017R01989

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF ONE SILVER IPHONE MODEL A1688 WIRELESS TELEPHONE WITH SERIAL NUMBER DNPQCTA2GRY9 CURRENTLY LOCATED IN SUFFOLK COUNTY, NEW YORK, IN THE CUSTODY OF THE DEPARTMENT OF HOMELAND SECURITY	APPLICATION FOR A SEARCH WARRANT FOR AN ELECTRONIC DEVICE Case No. MJ - 18 310

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH

I, DEBRA GERBASI, being first duly sworn, hereby depose and state as follows:

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of one silver iPhone model A1688 wireless telephone with serial number DNPQCTA2GRY9 currently located in Suffolk County, New York, in the custody of the Department Of Homeland Security—an electronic device (the "SUBJECT DEVICE")—that is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

DEFINITIONS

2. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. "Child Erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

b. "Child Pornography," as used herein, includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct), as well as any visual depiction, the production of which involves the use of a minor engaged in sexually explicit conduct (see 18 U.S.C. §§ 2252 and 2256(2)).

c. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

d. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. See 18 U.S.C. § 2256(2).

e. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1). The definition of a "computer" pursuant to Title 18, United States Code, Section 1030(e)(1) includes devices which may be used to store digital images, such as wireless telephones, MP3 players, video game systems and digital cameras.

f. "Internet" refers to the global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

g. "Wireless telephone," or a mobile telephone, or cellular telephone, means a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

h. "Digital camera" means a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

i. "Portable media player" means a portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some

portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

j. "GPS" means a navigation device that uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

k. "PDA" means a personal digital assistant. A PDA is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software,

giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

l. "IP Address" means an Internet Protocol address. An IP Address is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

3. Based on my training, experience, I know that the SUBJECT DEVICE has capabilities that allows it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

PEER-TO-PEER

4. Peer to Peer (P2P) file sharing allows people using P2P software to download and share files with other P2P users using the same or compatible P2P software. P2P software is readily available on the Internet and often free to download. Internet connected devices such as computers, tablets and smartphones running P2P software form a P2P network that allow users on the network to share digital files.

5. The BitTorrent network is a very popular and publically available P2P file sharing network. A peer/client computer can simultaneously provide files to some peers/clients while downloading files from other peers/clients. The BitTorrent network can be accessed by peer/client computers via many different BitTorrent network programs, examples of which include the BitTorrent client program, uTorrent client program, and Vuze client program, among others.

6. During the installation of typical BitTorrent network client programs, various settings are established which configure the host computer to share files via automatic uploading. Typically, as users download files or pieces of files from other peers/clients on the BitTorrent network, other peers/clients on the network are able to download the files or pieces of files from them, a process which maximizes the download speeds for all users on the network.

7. Files or sets of files are shared on the BitTorrent network via the use of "Torrents." A Torrent is typically a small file that describes the file(s) to be shared. It is important to note that "Torrent" files do not contain the actual file(s) to be shared, but information about the file(s) to be shared. This information includes the "info hash," which is a SHA-1 hash value of the set of data describing the file(s) referenced in the Torrent. This set of data contains the SHA-1 hash value of each file piece in the Torrent, the file size(s), and the file name(s). This "info hash" uniquely identifies the Torrent file on the BitTorrent network.

8. In order to locate Torrent files of interest and download the files that they describe, a typical user will use keyword searches on Torrent-indexing websites, examples of which include *isohhunt.com* and the *piratebay.org*. Torrent-indexing websites do not actually host the content (files) described by Torrent files, only the Torrent files themselves. Once a Torrent file is located on the website that meets a user's keyword search criteria, the user will

download the Torrent file to their computer. The BitTorrent network client program on the user's computer will then process that Torrent file to help facilitate finding other peers/clients on the network that have all or part of the file(s) referenced in the Torrent file.

9. For example, a person interested in obtaining child pornographic images or videos on the BitTorrent network can go to a Torrent-indexing website and conduct a keyword search using a term such as "preteen sex" or "pthc" (pre-teen hardcore). Based on the results of the keyword search, the user would then select a Torrent of interest to them to download to their computer from the website. Typically, the BitTorrent client program will then process the Torrent file. Utilizing BitTorrent network protocols, peers/clients are located that have recently reported they have the file(s) or parts of the file(s) referenced in the Torrent file and that these file(s) are available for sharing. The user can then download the file(s) directly from the computer(s) sharing them. Typically, once the BitTorrent network client has downloaded part of a file(s), it may immediately begin sharing the file(s) with other users on the network. The downloaded file(s) are then stored in an area or folder previously designated by on the user's computer or on an external storage media. The downloaded file(s), including the Torrent file, will remain in that location until moved or deleted by the user and are available for sharing to other BitTorrent users.

10. Law enforcement can search the BitTorrent network in order to locate individuals sharing child pornography images, which have been previously identified as such based on their SHA1 values. Law enforcement uses BitTorrent network client programs which allow for single-source downloads from a computer at a single IP address, meaning that an entire file(s) is downloaded only from a computer at a single IP address as opposed to obtaining the file from multiple peers/clients on the BitTorrent network. This procedure allows for the detection and

investigation of those computers involved in sharing digital files of known or suspected child pornography on the BitTorrent network.

11. Accordingly, in order to effectively use a P2P client software using the BitTorrent protocol, a user is making several pieces of information publically available to all other users of the P2P network: (1) the IP address of his/her computer, which is necessary to share files between computers on the network (like a delivery address); (2) that the user's computer is employing a particular P2P client program (here, a BitTorrent program); (3) confirmation from the suspect client that they have pieces of the file(s) being requested, in whole or in part, and that the pieces of the file(s) is being reported as available for sharing from the suspect client program; and (4) the content of any files a user is sharing via that P2P program, which the user – either by default, or by selection – has made available for other users to download through the P2P network. Law enforcement can then log this information.

12. The investigation of P2P file sharing networks is a cooperative effort of law enforcement agencies around the country. Many of these agencies are associated with the Internet Crimes against Children (ICAC) Task Force Program. The ICAC Task Force Program uses law enforcement tools to track IP addresses suspected (based on SHA1 values and file names) of trading child pornography. P2P investigative methodology has reliably led to the issuance and execution of numerous search warrants around the country resulting in the location of evidence, arrest and conviction of offenders possessing and/or trafficking in child pornography.

13. The computers that are linked together to form the P2P network are located throughout the world; therefore, the P2P network operates in interstate and foreign commerce.

PROBABLE CAUSE

14. Beginning on or about April 19, 2017, using P2P software developed for law enforcement use (which accesses information publicly available to anyone using the BitTorrent network) to identify users sharing child pornography files with others, I sought to identify BitTorrent users actively sharing child pornography on Long Island. Using this BitTorrent P2P software, a number of Long Island towns were selected. Thereafter, the P2P software program sought to download files previously identified as being of investigative interest to child pornography investigations from users located at IP Addresses that are believed to be geographically located on Long Island.

15. Between April 19, 2017 and September 19, 2017, the BitTorrent P2P software and database downloaded hundreds of files previously identified as being of investigative interest to child pornography investigations on approximately thirty-seven (37) occasions from a computer of internet device(s) located at IP address 68.192.212.18. These files, which I reviewed, include both still images and videos, and include both child erotica and child pornography. Three of the child pornography files downloaded from IP address 68.192.212.18, which are available for the Court's review, are described as follows:

a. On or about June 6, 2017, the P2P BitTorrent software downloaded a video titled "2007 Tara 8Yr – collection-It hurts Daddy.wmv", which depicts a pre-pubescent girl lying on a bed and inserting her fingers into her vagina;

b. On or about June 6, 2017, the P2P BitTorrent software downloaded an image file titled "Pthc Ptsc Jenny 9Yo Daughter With Cum In Mouth, New.jpg" which depicts a young girl with a white substance in her mouth.

c. On or about April 19, 2017, the the P2P BitTorrent software downloaded an image file titled " pthc_ptsc jenny_my 9 yo naked.jpg" which depicts a pre-pubescent girl lying on a bed naked with her legs spread open.

16. Account information obtained from the Internet Service Provider Verizon relating to IP address 68.192.212.18 for the dates described above, this IP address was assigned to the account of "Joann Scanlon" at a premises later identified as the residence of NICHOLAS FIESEL (the "FIESEL RESIDENCE"). This account was active as of September 13, 2017 (the date of the Cablevision response) at said premises.

17. On October 26, 2017, the Honorable A. Kathleen Tomlinson , United States Magistrate Judge for the Eastern District of New York signed as search warrant (17-MC-931) for the search of the FIESEL RESIDENCE. On or about October 30, 2017, law enforcement executed a search of the FIESEL RESIDENCE. The search of the FIESEL RESIDENCE produced electronic devices owned and operated by FIESEL, which were found to contain child pornography and child erotica.

18. FIESEL was not in the FIESEL RESIDENCE at the time of the October 26, 2017 search. He subsequently agreed to speak to and meet with law enforcement. At the time, FIESEL was in the possession of the SUBJECT DEVICE.

19. Upon being interviewed by law enforcement, FIESEL admitted to downloading and distributing child pornography and to having done so for approximately 1-2 years. He also provided law enforcement with verbal consent to search the SUBJECT DEVICE. Upon obtaining that consent, I observed images that, in my training and experience, were consistent with images of child pornography. Based upon that cursory review, however, I cannot confirm that the images contain child pornography. The SUBJECT DEVICE was subsequently powered down on October 31, 2017 and inventoried as evidence. The SUBJECT DEVICE has remained off since that time.

20. On or about October 30, 2017, FIESEL was arrested. On October 30, 2017, FIESEL was arraigned on a Complaint charging him with the transportation of child pornography in violation of Title 18, United States Code, Section 2252(a)(1). On November 15, 2017, a grand jury sitting in the Eastern District of New York returned an Indictment charging FIESEL with transportation, receipt and possession of child pornography in violation of Title 18, United State Code, Sections 2252(a)(1), 2252(a)(2) and 2252(a)(4)(B), respectively (collectively, the "SUBJECT OFFENSES").

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

21. As noted, *supra*, "Computer" is used herein pursuant to the definition set forth in 18 U.S.C. § 1030(e)(1). This definition includes devices that may be used to store digital images, such as wireless telephones, MP3 players, video game systems and digital cameras.

22. Computers and computer technology have revolutionized the way in which individuals interested in child pornography perpetrate their crimes. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. There were definable costs involved with the production of pornographic images. To distribute these on any scale required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings and telephone calls.

23. The development of computers has changed this. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage. The computer's ability to store images in digital form makes the computer itself an

ideal repository for child pornography. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

24. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

25. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains peer to peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

OFFENDER CHARACTERISTICS

26. Over the course of my law enforcement career, I have conducted a significant number of investigations concerning child pornography. I have personally interviewed a large number of child sex offenders who committed online child pornography crimes, and have been informed of the studies of child sex offenders in general, and child pornography offenders in particular. I have learned about the activities and characteristics of child pornography offenders from other law enforcement agents who focus on online child sexual exploitation, including those who investigate such offenses and those who analyze the computer equipment of the offenders.

27. Based on my training and experience, I know that the following traits and characteristics are generally found to exist and be true in cases involving individuals who commit the SUBJECT OFFENSES:

a. The majority of individuals who commit the SUBJECT OFFENSES collect sexually explicit materials of children, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual gratification. The majority of these individuals also collect child erotica, which may consist of images or text that do not rise to the level of child pornography but which nonetheless fuel their deviant sexual fantasies involving children.

b. The majority of individuals who commit the SUBJECT OFFENSES seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance and support. This contact also helps these individuals to rationalize and validate their deviant sexual interest and associated behavior. The different Internet-based vehicles used by such

individuals to communicate with each other include, but are not limited to, P2P, e-mail, e-mail groups, bulletin boards, IRC, newsgroups, instant messaging, and other similar platforms.

c. The majority of individuals who commit the SUBJECT OFFENSES often collect, read, copy or maintain names, addresses (including e-mail addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange or commercial profit. These names may be maintained in the original medium from which they were derived, in telephone books or notebooks, on computer storage devices, or merely on scraps of paper.

d. The majority of individuals who commit the SUBJECT OFFENSES rarely dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft, and damage their collections of illicit materials.

28. Based on my own experience in investigating computer-facilitated child sexual exploitation crimes, and the experiences of other law enforcement agents with whom I have consulted, I believe that the majority of individuals who commit the SUBJECT OFFENSES via the Internet maintain images they obtain, increasingly in both online and offline storage media, as well as on hard drives of devices and in cloud or other types of virtual or remote storage locations. Doing so allows them to access and maintain their contraband even as they move from one physical location to another.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

29. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the

Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

30. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the SUBJECT DEVICE was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the SUBJECT DEVICE because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

b. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

c. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the

application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

d. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

31. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrants I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

32. Manner *of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

33. I submit that this affidavit supports probable cause for search warrants authorizing

the examination of the SUBJECT DEVICE described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

Debra Gerbasi
Special Agent
Department of Homeland Security

Subscribed and sworn to before me
on April 10, 2018:

/s/ STEVEN I. LOCKE

THE HONORABLE STEVEN I. LOCKE
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

The property to be searched is one silver iPhone model A1688 wireless telephone with serial number DNPQCTA2GRY9 currently located in Suffolk County, New York, in the custody of the Department of Homeland Security (the "SUBJECT DEVICE"). This warrant authorizes the forensic examination of the SUBJECT DEVICE for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

ITEMS TO BE SEIZED

A. Images of child pornography or child erotica; files containing images; and data of any type relating to the sexual exploitation of minors, in any form;

B. Visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors;

C. Stories, text-based files, motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors;

D. Information, correspondence, records, documents or other materials pertaining to the possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, or pertaining to the sexual exploitation of minors, that were transmitted or received using computer, cellular device, personal digital assistant, or some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail including, but not limited to:

   a. Correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors; and

   b. Records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors;

E. Any and all records, documents, or materials, including any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate commerce including by United States mail or by computer, any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256 or relating to the sexual exploitation of minors;

F. Any and all records, documents, or materials, including any and all address books, names, and lists of names and addresses of minors visually depicted while engaging in sexually explicit conduct, defined in Title 18, United States Code, Section 2256; or relating to the sexual exploitation of minors;

G. Any and all records of Internet usage including user names and e-mail addresses and identities assumed for the purposes of communication on the Internet. These records may include billing and subscriber records, chat room logs and e-mail messages;

H. Files, records, programs, logs, electronic communications, scanning programs, financial records, hacking software, or router configuration software;

I. Credit card information including but not limited to bills and payment records, including but not limited to records of internet access;

J. Any data or materials establishing ownership, use or control of any computer equipment seized.